## IN THE CLAIMS

Claim 1 has been amended as follows:

1.    (Currently Amended)   A method for protecting a device against operation with unauthorized consumables, comprising the steps of:

(a) generating a device identification number and uniquely allocating said device identification number to a device;

(b) generating a code number range, containing a plurality of code numbers, and allocating said code number range to said device identification number;

(c) generating a reference code number range, containing a plurality of reference code numbers respectively having relationships to the respective code numbers in said code number range;

(d) storing said device identification number and said reference code number range in said device;

(e) aggregating a code number in said code number range with a replacement consumable;

(f) recognizing a need to replace a depleted consumable in said device;

(g) before substituting said replacement consumable for said depleted consumable in said device, authenticating said replacement consumable by entering said code number aggregated with said replacement consumable into said device and, in said device, obtaining an authentication result by checking whether said code number aggregated with said replacement consumable has said relationship to one of said reference code numbers in said reference code number

range stored in said device and, if so, consuming said one of said reference code numbers in said device by ~~striking~~ <u>permanently deleting</u> said one of said reference code numbers from said device; and

(h) controlling said device dependent on said authentication result.

2. (Original) A method as claimed in claim 1 wherein step (h) comprises allowing substitution of said depleted consumable with said replacement consumable if said code number aggregated with said replacement consumable has said relationship to one of said reference code numbers in said reference code number range stored in said device.

3. (Original) A method as claimed in claim 1 comprising disallowing operation of said device with said replacement consumable if said code number aggregated with said replacement consumable does not have said relationship to one of said reference code numbers in said reference code number range stored in said device.

4. (Original) A method as claimed in claim 1 wherein step (h) comprises allowing operation of said device in a modified manner with said replacement consumable if said code number aggregated with said replacement consumable does not have said relationship to one of said reference code numbers in said reference code number range stored in said device.

5. (Original) A method as claimed in claim 1 comprising the additional steps of:

storing the allocation of the device identification number to said code number range in a data bank at a data center remote from said device;

storing the code number aggregated with said replacement consumable in said data bank associated with said code number range and said device identification number allocated thereto; and

upon each recognition of a need to replace a depleted consumable in said device, and if said code number has not been entered into said device, establishing a communication between said device and said remote data center to inform said remote data center of said need to replace said depleted consumable, and monitoring usage of the consumable represented by said depleted consumable at said remote data center.

6. (Original)  A method as claimed in claim 5 comprising accumulating data in said device related to usage of said depleted consumable and, after establishing communication between said device and said remote data center, transmitting said data from said device to said remote data center for use in said monitoring.

7. (Original)  A method as claimed in claim 6 wherein said data include an indication if and when all of said reference code numbers in said reference code range stored in said device have been consumed.

8. (Original)  A method as claimed in claim 7 comprising the additional step of, upon receiving said indication at said remote data center, transmitting a new reference code number range from said remote data center to said device and reloading said new reference code number range into said device.

9.     (Original)     A method as claimed in claim 7 comprising the additional step of, upon receipt of said indication at said remote data center, transmitting a new group of reference code numbers from said remote data center to said device and reloading said new group of reference code numbers into said device.

10.     (Original)     A method as claimed in claim 7 comprising the additional step of, upon receipt of said indication at said remote data center, producing a chip card having a new group of reference code numbers stored therein, physically transporting said chip card to said device, and inserting said chip card into a chip card reader at said device to load said new group of reference code numbers into said device.

11.     (Original)     A method as claimed in claim 1 wherein step (e) comprises aggregating said code number with said replacement consumable by storing said code number in a chip card and physically associating said chip card with said replacement consumable.

12.     (Original)     A method as claimed in claim 11 comprising additionally storing in said chip card a plurality of quantities related to usage of said replacement consumable during operation of said device.

13.     (Original)     A method as claimed in claim 1 wherein said device has a user interface, and wherein step (g) comprises entering said code number aggregated with said replacement consumable into said device via said user interface.

14. (Original)    A method as claimed in claim 13 wherein step (e) comprises permanently affixing said code number to said replacement consumable in a manner allowing said code number to be identified for entry into said device via said user interface.

15. (Original)    A method as claimed in claim 14 comprising affixing said code word to said replacement consumable dependent on a physical nature of said replacement consumable.

16. (Original)    A method as claimed in claim 1 wherein step (f) comprises monitoring consumption of said consumable in said device by indirectly measuring usage of said consumable, to determine when said consumable is depleted.

17. (Original)    A method as claimed in claim 1 comprising conducting step (b) at a manufacturer of said replacement consumable, and wherein step (e) comprises aggregating said code number in said code number range with said replacement consumable during manufacture of said replacement consumable.

Claim 18 has been amended as follows:

18. (Currently Amended)    In a device which consumes a consumable during operation thereof, the improvement of an arrangement for protecting said device against operation with an unallowed consumable, said arrangement comprising:

at least one sensor for monitoring usage of a consumable in a device, said sensor emitting a sensor signal;

a microprocessor in said device supplied with said sensor signal and identifying a need for replacement of said consumable before actual replacement of said consumable is necessary;

a display connected to said microprocessor, said microprocessor generating a message on said display indicating said need for replacing said consumable;

a memory accessible by said microprocessor in which a reference code number range is stored, said reference code number range containing a plurality of reference code numbers respectively having relationships to code numbers representing an authorized replacement consumable;

an input unit connected to said microprocessor, said microprocessor, upon generating said message, waiting for entry, via said input unit, of a code number and, upon entry of said code number via said input unit, said microprocessor producing an authentication result dependent on whether said code number has said relationship to one of said reference code numbers in said memory and, if so, causing said one of said reference code numbers to be consumed by ~~striking~~ permanently deleting said one of said one reference code numbers from said memory; and

said microprocessor controlling operation of said device dependent on said authentication result.

19. (Original) An arrangement as claimed in claim 18 wherein said device is a printing device having an inking ribbon in a cassette, as said consumable, and wherein said sensor comprises an encoder which interacts with said cassette.

20. (Original)    An arrangement as claimed in claim 18 wherein said sensor comprises a sensor for physically interacting with said consumable.

21. (Original)    An arrangement as claimed in claim 20 wherein said device comprises a printing device having an interchangeable ink tank cassette containing electrically conductive ink as said consumable, and wherein said sensor comprises electrical contacts interacting with said electrically-conductive ink to identify an amount of said electrically conductive ink in said ink tank cassette.

22. (Original)    An arrangement as claimed in claim 18 wherein said device comprises a printing device having an ink jet print head with an integrated ink tank containing ink, said ink comprising said consumable.

23. (Original)    An arrangement as claimed in claim 18 wherein said device comprises a device which consumes a liquid as said consumable, said liquid being packaged in packaging material having an identifier thereon usable as said code number.

24. (Original)    An arrangement as claimed in claim 18 wherein said device consumes a non-solid aggregate state consumable.

25. (Original)    An arrangement as claimed in claim 18 wherein said device consumes a solid consumable.

26. (Original)    An apparatus as claimed in claim 18 wherein said device is a postage meter machine having a printer which produces a plurality of franking imprints, thereby consuming said consumable, and wherein said microprocessor monitors a number of said franking imprints which occur between each replacement of said consumable, and wherein said microprocessor uses said number of franking imprints as a basis for producing said authentication result.

27. (Original) An arrangement as claimed in claim 22 wherein said microprocessor generates a message for display on said display if said authentication result indicates an unauthorized replacement.

28. (Original) An arrangement as claimed in claim 26 wherein said microprocessor establishes a communication to a remote location, dependent on said authentication result, upon triggering by an entry via said user interface.

29. (Original) An arrangement as claimed in claim 26 wherein said device has a modem connected thereto, and wherein said microprocessor automatically establishes said communication to a remote location, dependent on said authentication result, via said modem.

30. (Original) An arrangement as claimed in claim 26 wherein said device has a chip card reader connected to said microprocessor, said chip card reader receiving a chip card therein, and wherein said microprocessor establishes a communication to a remote location, dependent on said authentication result, upon insertion of said chip card into said chip card reader

31. (Original) An arrangement as claimed in claim 26 wherein said postage meter machine requires periodic credit reloading, and wherein said microprocessor establishes a communication to a remote location in conjunction with a credit reloading and reports said authentication result in said communication.

Claim 32 has been amended as follows:

32. (Currently Amended) A method for protecting a device against operation with unauthorized consumables, comprising the steps of:

(a) generating a device identification number and uniquely allocating said device identification number to a device;

-9-

(b) generating a code number range, containing a plurality of code numbers, and allocating said code number range to said device identification number;

(c) generating a reference code number range, containing a plurality of reference code numbers respectively having relationships to the respective code numbers in said code number range;

(d) storing said device identification number and said reference code number range in said device;

(e) aggregating a code number in said code number range with a replacement consumable;

(f) operating said device through a plurality of cycles with a consumable in said device that is incrementally depleted in each cycle, and recognizing a need to replace said consumable, as a depleted consumable, in said device by generating and storing a running count of an item associated with said incremental depletion over said plurality of cycles, and indicating a need to replace said consumable when said running count reaches a predetermined level;

(g) before substituting said replacement consumable for said depleted consumable in said device, authenticating said replacement consumable by entering said code number aggregated with said replacement consumable into said device and, in said device, obtaining an authentication result by checking whether said code number aggregated with said replacement consumable has said relationship to one of said reference code numbers in said reference code number

range stored in said device and, if so, consuming said one of said reference code numbers in said device by ~~striking~~ <u>permanently deleting</u> said one of said reference code numbers from said device; and

(h) controlling said device dependent on said authentication result.

33. (Previously Presented) A method as claimed in claim 32 wherein said device is a printer for printing franking imprints and wherein said item count is a number of said franking imprints.

Claim 34 has been amended as follows:

34. (Currently Amended) A method for protecting a device against operation with unauthorized consumables, comprising the steps of:

(a) generating a device identification number and uniquely allocating said device identification number to a device;

(b) generating a code number range, containing a plurality of code numbers, and allocating said code number range to said device identification number;

(c) generating a reference code number range, containing a plurality of reference code numbers respectively having relationships to the respective code numbers in said code number range;

(d) storing said device identification number and said reference code number range in said device;

(e) aggregating a code number in said code number range with a replacement consumable;

(f) recognizing a need to replace a depleted consumable in said device;

-11-

(g) before substituting said replacement consumable for said depleted consumable in said device, authenticating said replacement consumable by entering said code number aggregated with said replacement consumable into said device and, in said device, obtaining an authentication result by checking whether said code number aggregated with said replacement consumable has said relationship to one of said reference code numbers in said reference code number range stored in said device and, if so, consuming said one of said reference code numbers in said device by ~~striking~~ permanently deleting said one of said reference code numbers from the reference code number range stored in said device; and

(h) controlling said device dependent on said authentication result.

Claim 35 has been amended as follows:

35.     (Currently Amended)    A method for protecting a device against operation with unauthorized consumables, comprising the steps of:

(a) generating a device identification number and uniquely allocating said device identification number to a device;

(b) generating a code number range, containing a plurality of code numbers, and allocating said code number range to said device identification number;

(c) generating a reference code number range, containing a plurality of reference code numbers respectively having relationships to the respective code numbers in said code number range;

-12-

(d) storing said device identification number and said reference code number range in said device;

(e) aggregating a code number in said code number range with a replacement consumable;

(f) determining a presence of a consumable in said device by detecting an occurrence of an event associated with depletion of said consumable;

(g) recognizing a need to replace said consumable, as a depleted consumable, in said device;

(h) before substituting said replacement consumable for said depleted consumable in said device, authenticating said replacement consumable by entering said code number aggregated with said replacement consumable into said device and, in said device, obtaining an authentication result by checking whether said code number aggregated with said replacement consumable has said relationship to one of said reference code numbers in said reference code number range stored in said device and, if so, consuming said one of said reference code numbers in said device by ~~striking~~ permanently deleting said one of said reference code numbers from said device; and

(i) controlling said device dependent on said authentication result.

36.     (Previously Presented)  A method as claimed in claim 35 wherein said event is reactivation of said device after shutdown of said device.

37.    (Previously Presented)  A method as claimed in claim 35 wherein said device is a thermal printer and wherein said consumable is a cassette containing a thermal transfer inking ribbon that is transported in said cassette by a first length for printing an image and that is transported by a second length, substantially smaller than said first length, between printing of successive images, and wherein said event is transport of said thermal transfer inking ribbon by said second length.